

## CLAIMS

1. A logic circuit for multiplication of an  $(m \times n)$  matrix by a  $(1 \times n)$  or by a  $(m \times 1)$  matrix, where  $m$  is a number of rows and  $n$  is a number of  
5 columns, and wherein each successive row  $m$  of  $n$  elements is a predetermined row permutation of a preceding row, the circuit comprising:

$n$  multiplication circuits (60...63) each having an input and an output which returns the value of said input multiplied by a predetermined multiplicand;

10  $n$  logic circuits, (70...73) each for executing a predetermined logical combination of a first input and a second input to provide a logical output, the first input being coupled to the output of a corresponding one of the  $n$  multiplication circuits;

$n$  registers (80...83) for receiving said logical output;

15 feedback logic for routing the contents of each register to a selected one of the second inputs in accordance with a feedback plan that corresponds to the predetermined row permutation; and

control means for successively providing as input to each of the  $n$  multiplication circuits each element in the  $(1 \times n)$  or  $(m \times 1)$  matrix.

20

2. The logic circuit of claim 1 in which the feedback logic provides a feedback plan corresponding to said predetermined row permutation that is a row shift.

25 3. The logic circuit of claim 2 in which the row shift is a single element right shift.

4. The logic circuit of claim 1 in which the  $n$  logic circuits are each adapted to execute an XOR-combination of said first input and said second  
30 input.

5. The logic circuit of claim 1 in which each of the predetermined multiplicands corresponds to one of the elements in the AES Rijndael MixColumns transform function.

5 6. The logic circuit of claim 5 in which the number  $m = 4$ , the number  $n = 4$ , the multiplicand for the first multiplication circuit = 02, the multiplicand for the second multiplication circuit = 03, the multiplicand for the third multiplication circuit = 01, and the multiplicand for the fourth multiplication circuit = 01.

10

7. The logic circuit of claim 5 in which the number  $m = 4$ , the number  $n = 4$ , the multiplicand for the first multiplication circuit = 0E, the multiplicand for the second multiplication circuit = 0B, the multiplicand for the third multiplication circuit = 0D, and the multiplicand for the fourth multiplication circuit = 09.

15

8. The logic circuit of claim 6 or claim 7 in which the four multiplicands are switchable between the values in claim 6 and the values in claim 7.

20

9. The logic circuit of claim 1 in which the control means is adapted to successively provide as input to each of the  $n$  multiplication circuits each successive element in the  $(1 \times n)$  or  $(m \times 1)$  matrix over each of  $n$  or  $m$  cycles of operation respectively.

25

10. The logic circuit of claim 1 in which each of the  $n$  multiplication circuits, each of the  $n$  logic circuits, and each of the  $n$  registers are at least eight bits wide.

30

11. The logic circuit of claim 1 in which the control means further includes means for providing as output from said logic circuit the contents of the  $n$  registers after each  $n$ th cycle.

12. The logic circuit of claim 1 in which the control means further includes means for resetting each of the registers prior to the first calculation cycle.

5

13. The logic circuit of claim 1 in which each successive row  $m$  of  $n$  elements is a predetermined row permutation of the immediately preceding row.

10

14. An AES MixColumns transform circuit incorporating the logic circuit of any one of claims 1 to 13.

15

15. An AES encryption and/or decryption engine incorporating the logic circuit of any one of claims 1 to 13 for performing the MixColumns transform.

16. Apparatus substantially as described herein with reference to the accompanying drawings.